

Levin x4948
TLF 05/07/2024

EXHIBIT A

**DECLARATION OF DAVID PANIWOZIK IN SUPPORT OF VERIFIED COMPLAINT
FOR FORFEITURE *IN REM***

I, David Paniwozik, a Special Agent with the Federal Bureau of Investigation (FBI) being duly sworn, state the following:

Introduction and Agent Background

1. I am a Special Agent with the FBI and have been since March 2020. As part of my duties, I investigate violations of federal law, including cyber-crime cases, computer and network intrusions, ransomware, cyber stalking, and internet fraud. I have gained experience in conducting such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I am currently assigned to the FBI Baltimore Cyber Task Force in Baltimore, Maryland. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. Prior to my employment as a Special Agent, I worked as a Forensic Accountant for the FBI in Chicago, Illinois from August 2017 to October 2019. During my time as a Forensic Accountant, I performed financial investigations, identified violations, and prepared legal exhibits. Further, I prepared and testified to exhibits as part of a federal trial.

PURPOSE OF THIS DECLARATION

3. This declaration is submitted in support of a complaint for forfeiture *in rem* of cryptocurrency funds seized from the following Binance accounts (collectively, the “**TARGET ACCOUNTS**”):

- **TARGET ACCOUNT 1:**

- **User ID:** 72164134
- **Associated Email Address:** isha.bhatia92@gmail.com
- **Wallet:** 1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE

- **TARGET ACCOUNT 2:**

- **User ID:** 91268389
- **Associated Email Address:** arjsai111184@gmail.com
- **Wallet:** 1HWQk7bREdiVMRsh1bCaFa5N5PDebrPVv3

4. The cryptocurrency amounts¹ seized from the **TARGET ACCOUNTS** on or about October 15, 2021 (the “Defendant Property”) are summarized in the below table:

TARGET ACCOUNT 1		
COIN	COIN NAME	QUANTITY
BTC	Bitcoin	2.001
ADA	Cardana	6,243.666
MATIC	Polygon	15,597.109
SHIB	SHIB INU	583,243,869.000
TRX	TRON	102,367.610
YFI	Yearn.finance	4.602
TLM	Alien Worlds	12,689.086

TARGET ACCOUNT 2		
COIN	COIN NAME	QUANTITY
USDT	Tether	151,503.480
DOGE	Dogecoin	1,136.305

5. I submit that there is probable cause to believe that all of the funds held in the **TARGET ACCOUNTS**, in any form, are proceeds of, or traceable to proceeds of violations of, inter alia, 18 U.S.C. §§ 1030(a)(4) (Unauthorized Access to a Protected Computer in Furtherance

¹ Unless otherwise noted, all cryptocurrency amounts in this declaration are rounded to the nearest .001.

of Fraud) and 1343 (Wire Fraud), and/or are involved in violations of, inter alia, 18 U.S.C. § 1956(a)(1)(B)(i) (Concealment Money Laundering), and therefore subject to civil forfeiture pursuant to and 18 U.S.C. § 981(a)(1)(A), (a)(1)(C), and (a)(1)(D).

Summary of the Investigation

A. Cryptocurrencies and Transaction Analysis

6. Bitcoin (BTC) is a “cryptocurrency,” also known as “virtual currency.” Cryptocurrencies are not tied to any nation’s fiat currency. The owner of cryptocurrency is assigned a mathematical encryption key pair, consisting of a “public key” and a “private key,” with which to control the currency they own. The public key is also known as an “address,” is visible to the public, and allows members of the public to verify the owner of virtual currency and other information. Addresses are also used to send and receive cryptocurrency. A “wallet” can hold multiple addresses for a user, and an “account” can hold multiple wallets for a user. The private key also known as a “secret key,” is essentially a password used to execute cryptocurrency transactions. Secret keys are typically only shared with the owner of the address.

7. “Ethereum” is a cryptocurrency, or virtual currency, that utilizes a blockchain-based software program. Ethereum is the world’s second-largest cryptocurrency by market capitalization, behind Bitcoin.

8. “TetherUS” (USDT), also referred to a “Tether”, is a cryptocurrency purportedly backed by United States dollars. Tether was originally designed to always be worth \$1, and the company responsible for issuing Tether purportedly maintained \$1 in reserves for each Tether issued.

9. Cryptocurrency transactions can have multiple inputs and multiple outputs. While the ownership of any particular address or wallet can be anonymous, all transactions of

cryptocurrencies are recorded on a “blockchain,” which is a series of “blocks” of transactions that establishes a verifiable, transparent record of the movement of virtual currency. Blockchains in this context are viewable by the public—they show all transactions, but do not reflect who owns a particular address. As cryptocurrency transactions are processed, they are assigned a unique identifier on the blockchain called a transaction hash.

10. Cryptocurrency exchanges exist and operate similarly to fiat currency exchanges. Customers use these exchanges to trade one form of digital currency for another, or to exchange digital currency into fiat money. Based on my training, knowledge, and experience, fraudsters often use cryptocurrency exchanges to launder or obfuscate their illicit gains.

11. Binance Holdings Limited (“Binance”) is a non-U.S. company registered in the Cayman Islands, which the U.S. Government has confirmed with Cayman authorities. Binance owns and operates Binance.com, a cryptocurrency exchange that provides a platform for trading various cryptocurrencies and exchanging cryptocurrencies for “fiat” (government-backed) currencies. Binance is one of the largest cryptocurrency exchanges in the world in terms of trading volume. Among other services, Binance provides customers with “custodial wallets,” meaning that Binance maintains the private keys relating to the customer’s cryptocurrency and therefore has complete control over client funds. Binance is therefore able to seize and transfer customer funds pursuant to legal process and court orders.

12. Based on my training and experience, financial account information, including cryptocurrency wallets, is not typically shared across multiple, unrelated individuals. I know from my training and experience that this shared use of information is very often the same person or a close and trusted group working in concert.

13. Based on my training and experience, I know that individuals engaged in criminal activity involving cryptocurrency frequently engage in “chain hopping,” meaning that they convert funds from one cryptocurrency to another, in order to obscure the source of funds and make it more difficult to track illicit funds as they move from one blockchain to another.

B. “Tech Support” Scams

14. In and around June and July 2021, The FBI investigated a technical-support scam involving elderly victims. Technical-support scams are perpetrated in several ways. In some instances, fraudsters make telephone calls and claim to be computer technicians associated with a well-known company. They will also use fake websites to generate internet pop-up messages that warn about non-existent computer problems. The messages will claim to have detected viruses or other malware on the victim’s computer that was placed there by hackers and will instruct users to contact a phone number for a “support line.”

15. When the victim calls the number provided, the fraudsters pretend to act as “tech support” and ask the victim to provide them with remote access to the victim’s computer and/or phone. This is typically accomplished by having the victim download a remote access application, such as TeamViewer or UltraViewer, which allows the fraudsters to remotely access the victim’s devices and review the data contained therein, such as bank account numbers and other identifying information.

16. Once the fraudsters have access to the victim’s computer, they will then act as if they are performing a diagnosis of the purported problem and will inform the victim that the victim’s computer, and personally identifiable information stored on it, has been compromised. The fraudsters will then ask the victim which financial institutions the victim has accounts with. When the victim provides this information, the fraudsters advise that these accounts may have

been compromised, and the victim will need to work with a bank representative to “clean” the accounts. The “tech support” fraudster transfers the victim to another fraudster, who will claim to be part of the “fraud department” at the victim’s financial institution.

17. Following this transfer, the “fraud department” fraudster explains to the victim that the victim’s bank account has been compromised. The fraudster then explains that, in order to “clean” the account, all of the funds must be transferred to a cryptocurrency exchange. The fraudster will set up or work with the victim to set up an account with the cryptocurrency exchange in the victim’s name. The victim is then told to conduct wire transfers to the cryptocurrency account or, in some cases, to another bank account that is connected to a cryptocurrency exchange and that the fraudsters have created in the victim’s name. The fraudsters ensure that the victim is always logged into a remote desktop software in order to monitor the activity and obtain verification codes.

18. Once the victim wires funds into the specified account(s), the fraudsters, without the victim’s knowledge, transfer the money to wallets controlled entirely by the fraudsters. This process is repeated several times until the victim has no more funds to transfer. Once the funds have been exhausted, the fraudsters stop all communication with the victim.

C. Victim A

19. The FBI investigated a technical fraud scam against “Victim A,” an individual located in Queenstown, Maryland. On or about the morning of June 9, 2021, after using a computer to browse the internet, several pop-up windows began to appear on the screen. Victim A also heard a woman talking and screaming sounds coming from the computer. One of the pop-up windows stated that the computer had been hacked and to contact Microsoft at 970-465-0878 for assistance. Victim A contacted the number on the screen.

20. An unknown male (“Fraudster 1”) answered the phone and identified himself as working for Microsoft. Victim A informed Fraudster 1 that it was difficult to hear him due to the noise coming from the computer. At some point during the call, Fraudster 1 used remote desktop software to access Victim A’s computer and stop the sound that had been playing. Fraudster 1 then told Victim A to log into Victim A’s bank accounts so he could run “tests.”

21. Once logged into Victim A’s bank accounts, Fraudster 1 told Victim A that he identified two fraudulent charges totaling approximately \$90,000. Fraudster 1 told Victim A that Victim A needed to contact Victim A’s bank to get this matter resolved. Fraudster 1 then provided a telephone number purported to be for Victim A’s Bank (315-758-4343), and he instructed Victim A to enter “000” after connecting. Victim A ended the conversation with Fraudster 1 and called the number provided.

22. The call was answered by another unknown male (“Fraudster 2”). Fraudster 2 informed Victim A again that there were two charges on Victim A’s account totaling approximately \$90,000. Fraudster 2 said that these charges were going to Russia. When Victim A told Fraudster 2 that Victim A did not see these charges in the account, Fraudster 2 responded that this was due to an issue with Victim A’s account. Fraudster 2 also stated that he would work to remove the transactions and that in order to do this, he would need to convert Victim A’s money to Bitcoin. Fraudster 2 stated that any losses to the funds would be covered by the Federal Reserve.

23. During this time, Fraudster 2 created two accounts in Victim A’s name: a Swan Bitcoin account (“Swan Dummy Account A”) and a Coinbase account (“Coinbase Dummy Account A”). The unknown male told Victim A that Victim A needed to wire out the money in Victim A’s bank account. The unknown male then sent a document to Victim A’s printer. The document included wire instructions, a reference number, and responses to any questions the bank

may ask. Victim A called Victim A's bank to conduct the wire transfer. After speaking with several individuals, Victim A's bank conducted the wire transfer. However, Victim A forgot to include the reference number on the wire. When Victim A contacted Fraudster 2 to inform him of the issue, Fraudster 2 said that he would work to track the wire down.

24. Fraudster 2 then accessed and utilized Victim A's email account. Representing himself as Victim A, Fraudster 2 communicated with Swan Bitcoin to track the wire transfer. Eventually, the wire transfer was located and deposited into Swan Dummy Account A.

25. Victim A wired approximately \$190,000 to Swan Dummy Account A. The fraudsters then transferred the funds to Coinbase Dummy Account A. This resulted in the purchase of approximately 4.861 Bitcoin (BTC), which was valued at approximately \$235,993 as of August 24, 2021. From there, the fraudsters transferred the funds from Coinbase Dummy Account A to a separate wallet used by the fraudsters that was not in Victim A's name.

DATE	AMOUNT	SOURCE	DESTINATION
6/16/2021	4.861 BTC	Swan Dummy Account A	Coinbase Dummy Account A

26. Pursuant to legal process, Coinbase provided information regarding Coinbase Dummy Account A. Analysis of the account identified that once the deposit from Swan Dummy Account A was received, the fraudsters immediately transferred the funds out of Coinbase Dummy Account A. The fraudsters sent Victim A's funds to the following wallet (BTC rounded to .001):

DATE	AMOUNT	SOURCE	DESTINATION
6/16/2021	4.861 BTC	Coinbase Dummy Account A	"Wallet 1" 1NzUwwHfbNVFDpHP8SJxW98x64DgqyNHqk

27. Through the use of commercially available tools, a tracing analysis was conducted on the withdrawal transaction. As set forth above, on June 16, 2021, 4.861 BTC from Victim A's

Coinbase account was transferred to **Wallet 1**. The 4.861 BTC was then combined with additional amounts from Wallet 1 and was immediately transferred to **TARGET ACCOUNT 1** on the same transactional hash:

DATE	AMOUNT	SOURCE	DESTINATION
6/16/2021	4.861 BTC	Wallet 1	TARGET ACCOUNT 1 1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE

28. Investigators contacted Binance and requested records associated with the “1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE” address. In response, Binance produced account records for the user who owned the “1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE” address, which included the following information:

USER ID	72164134
NAME	Isha Bhatia
EMAIL	isha.bhatia92@gmail.com
MOBILE/SMS	+919873265028
REGISTRATION TIME	2021-01-31 04:25:05

29. As proof of identity, the user sent Binance an image of a Government of India Unique Identification Card, or Aadhaar Card, in the name of Isha Bhatia, reflecting a date of birth in February 1992. The user also sent an image purported to be a picture of herself. Usage data from Binance indicates that the user accessed the account from India using an Apple iOS device.

D. Victim B

30. The FBI also investigated a technical support fraud scam against “Victim B,” an individual located in Louisville, Kentucky. On June 3, 2021, while searching the internet, Victim B came across an article regarding movie stars. When Victim B attempted to open the article, Victim B’s computer started making a loud noise that sounded like a tornado siren. A pop-up message appeared on the screen purporting to alert Victim B that the computer had been hacked

and instructing Victim to contact Microsoft. The pop-up message provided a telephone number provided for Microsoft: 425-484-9861, extension 1011. Victim B called the number provided.

31. An unknown male (“Fraudster 3”)² answered the phone and identified himself as working for Microsoft. Victim B explained the issue to Fraudster 3, who then requested access to Victim B’s computer through the use of a remote desktop software. Once he had access, Fraudster 3 told Victim B to leave the computer on at all times.

32. Fraudster 3 then told Victim B that he needed to run diagnostics on the computer. He informed Victim B that based on his analysis, Victim B’s bank account had been compromised. Fraudster 3 stated that there were three fraudulent transactions on the account. Fraudster 3 asked Victim B for the telephone number on the back of Victim B’s bank card to call and offered to connect Victim B directly. Fraudster 3 told Victim B to ask to speak with someone in the fraud department.

33. Victim B was then connected with another unknown male who identified himself as working in the fraud department at Victim B’s bank (“Fraudster 4”). Fraudster 4 said there were three pending charges against Victim B’s account. The transactions totaled approximately \$40,000 and related to charges at a casino. Fraudster 4 told Victim B to log into Victim B’s bank account to confirm the amounts. Once Victim B logged in, Fraudster 4 told Victim B that he needed to secure all of Victim B’s accounts. He said Victim B’s money market account, Individual Retirement Account (IRA) and Certificate of Deposit (CD) accounts had all been compromised.

² The unknown males who spoke with all the victims may have been the same two men that spoke with Victim A (Fraudsters 1 and 2). However, due to the lack of certainty as to how many individuals are involved in the fraudulent schemes, this declaration refers to the specific men that spoke with each victim as unique individuals.

Fraudster 4 then stated he would place Victim B on hold because he needed to contact the Federal Reserve for next steps.

34. Fraudster 4 then returned to the call to inform Victim B that he would need to secure the funds in Bitcoin. During this time, Fraudster 4 walked Victim B through the process of setting up accounts with Swan Bitcoin (“Swan Dummy Account B”) and Coinbase (“Coinbase Dummy Account B”).

35. Following the creation of Swan Dummy Account B and Coinbase Dummy Account B, the fraudsters called Victim B every day for approximately one month. The fraudsters provided Victim B with instructions to conduct financial transactions from Victim B’s financial accounts. Over the course of six weeks, Victim B wired approximately \$421,000 to a Swan Dummy Account B. After funds were deposited in Swan Dummy Account B, the fraudsters then transferred the funds to Coinbase Dummy Account B. This resulted in the purchase of approximately 11.775 Bitcoin (BTC), which was valued at approximately \$577,665 as of August 24, 2021. From there, the fraudsters transferred the funds from Coinbase Dummy Account B to separate wallets used by the fraudsters that were not in Victim B’s name.

36. Pursuant to legal process, Coinbase provided information regarding Coinbase Dummy Account B. Analysis of the account identified the following four deposits from accounts controlled by Victim B to the Coinbase Dummy Account B:

DATE	AMOUNT	SOURCE	DESTINATION
6/22/2021	2.856 BTC	Swan Dummy Account B	Coinbase Dummy Account B
6/24/2021	3.529 BTC	Swan Dummy Account B	Coinbase Dummy Account B
7/1/2021	4.923 BTC	Swan Dummy Account B	Coinbase Dummy Account B
7/14/2021	0.467 BTC	Swan Dummy Account B	Coinbase Dummy Account B

TOTAL	11.775 BTC		
--------------	-------------------	--	--

37. Once the deposits were received in Coinbase Dummy Account B, the fraudsters immediately transferred the funds out of the account. Victim B's funds were sent to the following four wallets:

DATE	AMOUNT	SOURCE	DESTINATION
6/22/2021	2.856 BTC	Coinbase Dummy Account B	"Wallet 2": bc1qh78r3qmfj4q8e68zv47s32gtlqjqdua86c640d
6/24/2021	3.529 BTC	Coinbase Dummy Account B	"Wallet 3": bc1qa6m68zx68r7mj85r2h0sxfsprh8rnzn9kk5x2h
7/12/2021	4.923 BTC	Coinbase Dummy Account B	"Wallet 4": bc1qyun8au4gln979kuj5p6f7nnu2e4c2905attx6h
7/14/2021	0.467 BTC	Coinbase Dummy Account B	"Wallet 5": bc1qdxrhhq5mj8n0z38lk9d0ewngtjgyce8ar3tre5
TOTAL	11.775 BTC		

38. Through the use of commercially available tools, a tracing analysis was conducted on the withdrawal transactions. The tracing analysis of **Wallets 2, 3, and 4** showed that all the Bitcoin initially sourced from Victim B was immediately transferred from those wallets to a single new wallet as follows:

DATE	AMOUNT	SOURCE	DESTINATION
6/22/2021	2.856 BTC	Wallet 2	"Wallet 6": bc1qh78r3qmfj4q8e68zv47s32gtlqjqdua86c640d
6/24/2021	3.529 BTC	Wallet 3	"Wallet 6": bc1qa6m68zx68r7mj85r2h0sxfsprh8rnzn9kk5x2h
7/12/2021	4.923 BTC	Wallet 4	"Wallet 6": bc1qyun8au4gln979kuj5p6f7nnu2e4c2905attx6h
TOTAL	11.308 BTC		

39. Tracing analysis of **Wallet 6** identified additional deposits. On the dates listed below, these amounts were then combined with the Bitcoin derived from **Victim B's** funds and transacted on the same hash to **TARGET ACCOUNT 1**:

DATE	AMOUNT	SOURCE	DESTINATION
6/23/2021	3.856 BTC	Wallet 6	TARGET ACCOUNT 1 1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE
6/24/2021	3.529 BTC	Wallet 6	TARGET ACCOUNT 1 1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE
7/1/2021	9.108 BTC	Wallet 6	TARGET ACCOUNT 1 1L3Af1kZGfrUm3xcPAqZFSsWXp7D14ixkE

40. The records provided by Binance confirmed the receipt of the above funds into **TARGET ACCOUNT 1**. According to Binance records, the user of **TARGET ACCOUNT 1** converted the above amounts, which include the 11.308 BTC from **Victim B**, into TetherUS. The funds were then immediately transferred to an unattributed Tether address.

E. Victim C

41. The FBI also investigated a technical support fraud scam against “Victim C,” an individual located in Eliot, Maine. The pattern of this fraud followed the same basic pattern as the fraudulent scheme employed against Victims A and B.

42. On March 5, 2021, Victim C was searching the internet and received an alert that Victim C’s computer had been compromised. A pop-up message appeared instructing Victim C to contact Microsoft at 888-390-4190.

43. Victim C called the number and spoke to an unknown female who identified herself as working at Microsoft (“Fraudster 5”). Fraudster 5 informed Victim C that Victim C’s computer had been accessed by five scammers who compromised all of Victim C’s data. Fraudster 5 then asked Victim C to provide the name of Victim C’s bank. After Victim C provided that information, Fraudster 5 stated she was transferring Victim C to a representative in that bank’s fraud

department. Fraudster 5 told Victim C that she needed to transfer Victim C through a “secured line” because of the compromise.

44. Once transferred, an unknown male (“Fraudster 6”) answered and identified himself as working in the “fraud department” at Victim C’s bank. Fraudster 6 informed Victim C that Victim C’s accounts had been compromised. Fraudster 6 instructed Victim C to download and install remote desktop software onto Victim C’s computer and phone. Victim C was told that the software was needed because the process of recovering the bank accounts would require granting Microsoft and the bank access Victim C’s computer in order scan and clean the accounts. Fraudster 6 also informed Victim C that he would need to create a “dummy” account to secure the funds in Victim C’s bank.

45. Over the course of 17 weeks, Victim C would call or receive a call from the fraudsters every day of the week. Each day, fraudsters instructed Victim C to launch the remote desktop software on Victim C’s phone and computer, provide the passcodes, and leave the devices on and active all day. The fraudsters also requested that Victim C check in approximately every twenty minutes.

46. After instructing Victim C to conduct an initial set of wire transfers,³ the fraudsters used the remote access software to confirm and verify the bank accounts in Victim C’s name. Victim C was then provided with instructions to conduct transactions from Victim C’s financial accounts. Over the course of approximately 15 weeks, Victim C wired approximately \$450,000 to a Swan Bitcoin account created by the fraudsters in Victim C’s name (“Swan Dummy Account

³ Before following the previously observed pattern of using “Swan Dummy” and “Coinbase Dummy” accounts, the fraudsters instructed Victim C to conduct wire transfers to a foreign bank account. In total, Victim C transferred approximately \$150,000 to a foreign bank account, at which point Victim C’s bank refused to allow further similar wire transfers.

C”). The fraudsters then transferred the funds to a Coinbase account they had created in Victim C’s name (“Coinbase Dummy Account C”). Those transfers ultimately resulted in the purchase of approximately 10.286 BTC, valued at approximately \$499,367 as of August 24, 2021.

47. Pursuant to legal process, Coinbase provided information regarding the account created in the name of Victim C. Analysis of the account identified the following four deposits from Swan Dummy Account C to Coinbase Dummy Account C:

DATE	AMOUNT	SOURCE	DESTINATION
4/14/2021	0.797 BTC	Swan Dummy Account C	Coinbase Dummy Account C
4/21/2021	2.704 BTC	Swan Dummy Account C	Coinbase Dummy Account C
5/17/2021	2.290 BTC	Swan Dummy Account C	Coinbase Dummy Account C
6/2/2021	4.495 BTC	Swan Dummy Account C	Coinbase Dummy Account C
TOTAL	10.286 BTC		

48. Once the deposits arrived in Coinbase Dummy Account C, the fraudsters immediately transferred funds out of the account. Victim C’s funds were sent to the following four wallets:

DATE	AMOUNT	SOURCE	DESTINATION
4/14/2021	0.797 BTC	Coinbase Dummy Account C	“ Wallet 7 ”: 15RUqPBbhpjZcNtwhnmUPQzsoV5cf34Qd
4/21/2021	2.704 BTC	Coinbase Dummy Account C	“ Wallet 8 ”: 1D8mz1keJKuX7192o8uRqdKfUsCmGKDaVo
5/17/2021	2.290 BTC	Coinbase Dummy Account C	“ Wallet 9 ”: 1P1KJ6e2ed5zYQS9BLNHXX7vLNTMJvtUuX
6/3/2021	4.495 BTC	Coinbase Dummy Account C	“ Wallet 10 ”: 1JJ9w4Zhqxgh8YzFf9b4FLWoXZ6GeXStvd

49. As set forth above, on June 3, 2021, 4.495 BTC from Coinbase Dummy Account C was transferred to **Wallet 10**. Analysis of **Wallet 10** showed that the 4.495 BTC from Victim C transacted on the same hash as 4.319 BTC from an unattributed wallet. This transaction hash conducted the following transfers:

DATE	AMOUNT	SOURCE	DESTINATION
6/16/2021	7.000 BTC	Wallet 10	TARGET ACCOUNT 2: 1HWQk7bREdiVMRsh1bCaFa5N5PDebrPVv3
6/16/2021	1.814 BTC	Wallet 10	Unattributed Wallet: bc1qk8qy9qg09shx2f4n9x65psdjhutwe54ysjhy52

50. Tracing analysis indicated that **TARGET ACCOUNT 2** was held at Binance. In response to legal process, Binance provided customer information associated with **TARGET ACCOUNT 2**, which included the following information:

USER ID	91268389
NAME	Arjun Saini
EMAIL	arjsai111184@gmail.com
REGISTRATION TIME	2021-03-02 09:41:55

51. As proof of identity, the user sent Binance an image of a Government of India Unique Identification Card, or Aadhaar Card, in the name of Arjun Saini, with a date of birth in November 1984. The Aadhaar Card number was 7144 5482 3061. The user also sent an image purported to be a picture of himself. Usage data from Binance indicates that the user accessed the account from India.

F. Seizures of Funds in the TARGET ACCOUNTS

52. On September 8, 2021, the Honorable J. Mark Coulson, United States Magistrate Judge for the District of Maryland, issued a warrant authorizing the seizure of funds from **TARGET ACCOUNT 1** and **TARGET ACCOUNT 2**. The FBI served Binance with the seizure

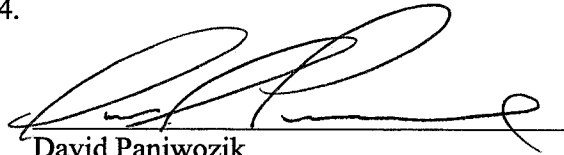
warrant shortly thereafter, and the contents of **TARGET ACCOUNT 1** and **TARGET ACCOUNT 2** were transferred into FBI custody on or about October 15, 2021.

CONCLUSION

53. Based on the forgoing, I submit that there is probable cause to believe that all of the funds held in the **TARGET ACCOUNTS**, in any form, are proceeds of, or traceable to proceeds of violations of, inter alia, 18 U.S.C. §§ 1030(a)(4) (Unauthorized Access to a Protected Computer in Furtherance of Fraud) and 1343 (Wire Fraud), and/or are involved in violations of, inter alia, 18 U.S.C. § 1956(a)(1)(B)(i) (Concealment Money Laundering), and therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), (a)(1)(C), and (a)(1)(D).

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct to the best of my knowledge, information and belief.

Executed this 7th day of May, 2024.

A handwritten signature in black ink, appearing to read 'David Paniwozik', is written over a horizontal line.

David Paniwozik
Special Agent
Federal Bureau of Investigation